Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Scienze di Internet

Il controllo della posta elettronica e dell'utilizzo delle risorse informatiche da parte dei lavoratori nella giurisprudenza dell'Autorità Garante per la protezione dei dati personali

Tesi di Laurea in Diritto di Internet

Relatore:
Chiar.mo Prof.
Giusella Finocchiaro

Presentata da:
Francesca Pugliese

Sessione II
Anno Accademico 2009/2010

Capitolo primo

1.1. Stato dell'arte

1.1.1 Cenni storici della disciplina della privacy

In questo capitolo si cercherà di ripercorre l'evoluzione storica della disciplina della riservatezza dei dati personali, comunemente denominata "*Privacy*".

In particolare verranno analizzate le modalità attraverso le quali, nel corso degli anni, la materia ha subito notevoli mutamenti da un punto di vista sia normativo, sia giurisprudenziale.

La genesi della "*Privacy*" si può certamente rinvenire negli accordi di Schengen[1] che vennero firmati il 14 giugno del 1985 nella città di Shengen, provincia Lussemburghese.

Gli stati che aderirono sin da subito furono solamente cinque: Belgio, Lussemburgo, Francia, Germania, Paesi Bassi, e solo in seconda istanza presero parte all'accordo altri stati europei, tra cui la stessa Italia il 27 novembre 1990.

---

1 Sito web: http://it.wikipedia.org/wiki/Accordi_di_Schengen

Stati Schengen con trattato in vigore

Stati Schengen con trattato non ancora in vigore

Microstati che adottano Schengen attraverso un accordo con un paese membro.

Stati dell'UE che non hanno adottato Schengen.

Figura 1: *stati europei e trattato di Shengen*

Gli accordi prevedevano da un lato l'abolizione delle dogane nei paesi membri, dall'altro il rafforzamento dei controlli al di fuori dei confini dovuto ad una maggiore cooperazione delle forze di polizia tra i vari stati, nonché all'integrazione delle banche dati delle stesse forze armate.

Lo scopo iniziale del trattato di Shengen era quello di abbattere le barriere tra gli stati sottoscrittori al fine di ottenere un progresso economico, in seguito alla alla libera circolazione di persone e merci da uno stato membro ad un altro, senza la necessità di passare per una o più dogane, ottenendo di conseguenza un notevole abbassamento dei costi.

Con l'applicazione del trattato di Schengen, a seguito della libera circolazione di persone e merci, diventa naturale anche la circolazione a sua volta maggiormente "libera" di informazioni e dati personali, spesso sensibil.

Il rischio era quello di liberalizzare sì il settore economico all'interno dell'unione europea, ma senza porre attenzione alla circolazione di informazioni, naturalmente incrementata e fuori controllo in un contesto non regolamentato *ad hoc*.

La problematica in essere ha posto l'esigenza di provvedere quindi ad una maggiore disciplina per quanto concerne il trattamento di particolari informazioni, in particolare quelle sensibili.

Nasce così **la direttiva del 46/95/CE**[2], testo di riferimento a livello europeo in materia di dati personali.

---

[2] Sito web http://europa.eu/legislation_summaries/information_society/l14012_it.htm

Essa contiene un quadro normativo atto a disciplinare la tutela della vita privata e la libera circolazione dei dati personali all'interno dell'Unione Europea (UE).

L'ambito di applicazione della direttiva 46/95/CE fa riferimento a dati generati in modalità automatica (es. database informatico) o più generalmente a dati archiviati sotto varia forma sia tradizionale che digitale (es. archivi in formato cartaceo), e non fa riferimento alla vita domestica o personale del soggetto interessato.

E' così che ci si trova a dover introdurre il concetto di "***Privacy",*** termine inglese che viene tradotto letteralmente con il termine: "***Riservatezza".***

Due grandi sostenitori della legge sulla *privacy* furono due giovani avocati, **Brandeis Louis** e **Samuel Warren** [3]**,** che nel 1890 scrissero un *paper* famosissimo dal titolo: **"*The right to be left alone".***

Nell'ottocento, epoca in cui prende piede l'industrializzazione, dove i contadini lasciano i terreni per andare a lavorare in fabbriche, e dove i rapporti interpersonali si affievoliscono, nasce l'esigenza del pettegolezzo di sapere cosa succede al di fuori delle proprie mura domestiche.

Ed è proprio alla fine dell'ottocento che nacquero le prime macchine da stampa, che velocizzarono la diffusione dei quotidiani e quindi delle informazioni. Essi divulgavano notizie locali, nazionali e internazionali, e lasciavano spesso adito a pettegolezzi in merito a persone note, attività oggi denominata di "*gossip*". E fu proprio al fine

---

[3] Sito web http://www.diritto.it/art.php?page=3&file=/archivio/27344.html

di tutelare ciò che avveniva all'interno delle mura domestiche di coloro i quali venivano trattati nei primi giornali a diffusione nazionale che i due avvocati elaborarono il trattato ***"The right to be left alone"*** ovvero ***"Il diritto di essere lasciati soli - in pace".***

Nel 1960 il concetto di privacy fu così ripreso *da* ***Prosser***[4], che scrisse un articolo in merito che riscontrò un buon successo.

Secondo Prosser la privacy era costituita da quattro elementi fondamentali. In primo luogo viene descritto il diritto all'interesse di essere liberi. In secondo luogo viene affrontato il tema del diritto ad esseri gli unici a poter disporre della propria privacy mentre in terzo luogo si parla di diritto ad avere interessa nella propria reputazione, tematica ripresa e approfondita anche nella quarta ed ultima istanza.

Purtroppo le quattro fondamenta elaborate da Prosser non ebbero il consenso sperato, e a comprometterne definitivamente lo sviluppo fu soprattutto la corte suprema degli anni sessanta.

La materia fu poi ripresa nel 1964 da ***Blounstein***, che criticò l'approccio al problema di Prosser.

Blounstein dava un significato diverso di *privacy*, secondo cui essa doveva ritornare concettualmente unitaria poiché esprime un valore essenziale dell'uomo, e che di conseguenza si evidenzia in tutti gli ambiti normativi in cui a questo si fa riferimento.

Contribuirono, quindi, a completare quello che sarebbe diventato il concetto di *privacy* definitivo molti altri personaggi del diritto.

---

4 Sito web http://www.altrodiritto.unifi.it/ricerche/control/surace/cap2.htm

Tra questi vanno ricordati:

"Losner 1964", secondo cui la privacy doveva essere intesa come "***Human dignity".***

Per ***"Westin 1967"*** era intesa come richiesta di un individuo, di un gruppo, di istituzioni di determinare se e quando e come ed in quale misura l'informazione su di loro possa essere comunicata ad altri.

E ancora ***Mellon*** *che* vedeva la *privacy* anche come spazio fisico, in senso corporale.

Infine **Noan** secondo cui la *privacy* era essenzialmente un concetto dinamico e non statico. Dinamico poiché frutto di un'interazione tra i diritti informativi di parti differenti che devono in qualche modo collidere.

Come accennato in precedenza per *privacy* si intende ora il diritto alla riservatezza, ossia il diritto della persona ad impedire la divulgazione o il trattamento dei propri dati senza il proprio consenso. Molti dati, se collegati tra loro, generano informazioni preziose poiché sono in grado di ricostruire dettagli relativi alla sfera personale di un individuo, e potrebbero inequivocabilmente ledere l'immagine o la dignità del diretto interessato qualora non venissero utilizzati secondo determinate modalità, oggetto di suddetta regolamentazione.

La ***legge 675/1996***[5]***,*** a conclusione dell'iter legislativo portato a termine dalla commissione Mirabelli, va ad ampliare aspetti legislativi in materia di diritti della personalità, ampiamente trascurati nelle normative precedenti.

---

[5] Sito web http://www.garanteprivacy.it/garante/doc.jsp?ID=1343305

La legge in questione mira a valorizzare il diritto all'identità personale, alla raccolta ed elaborazione d'informazioni a carattere personale, nonché al trattamento di esse.

I soggetti sottoposti al trattamento devono essere avvisati e delucidati sul fine dell'elaborazione dei propri dati prima ancora che essi vengano elaborati.

Questo concetto prende il nome di ***"Trasparenza dei dati".***

E' possibile affermare che per quanto riguarda l'autorizzazione al trattamento dei propri dati, si è passati da un modello statico a un modello dinamico.

Un modello dinamico, al contrario di uno di tipo statico, garantisce un continuo aggiornamento, correzione e accesso ai dati.

L'interessato può in qualunque istante verificarne la correttezza dell'elaborazione, in mondo tale da essere messo in condizione di avere potenzialmente una supervisione costante sui propri dati e negare o esprimere consenso laddove gli sembrerà opportuno.

Tuttavia, la legge **675/96** fu poco dopo abrogata con l'entrata in vigore del testo unico sulla privacy **D.lgs. 196/2003**, che ha così disciplinato in modo attualmente definitivo l'intera materia.

IL D.lgs 196/2003 è nato con l'intento di raccoglie e ordinare la variegata stesura legislativa e regolamentare, diventata di difficile comprensione e consultazione.

La struttura del D.lgs 196/2003 è organizzata sostanzialmente in tre parti.

La prima comprende le regole generali per il trattamento dei dati privati e pubblici, i diritti dell'interessato, dei soggetti che effettuano il trattamento, il dovere alla sicurezza dei dati unita ad altri adempimenti di varia natura, e ad una regolamentazione sul trasferimento all'estero.

La seconda parte contiene invece disposizioni precise in merito a particolari settori tra cui: giustizia, forze di polizia, sanità, istruzione, trattamenti per fini statistici e scientifici, settore bancario ed assicurativo, reti telematiche, giornalismo, investigazione privata, marketing privato.

La terza ed ultima parte viene interamente dedicata alla tutela dell'interessato e alle modalità con cui è possibile adempiere all'esercizio dei suoi diritti, non che ai compiti del Garante, alla struttura organizzativa dello stesso Garante, fino alla definizione delle modalità di sanzionamento in caso di inadempimento.

La finalità del D.lgs. 196/2003[6] è quella di garantire che il trattamento dei dati personali venga eseguito nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il D.lgs. 196/2003 all'art. 4 lettera "a" disciplina il termine "***trattamento"*** come qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la

---

6 Sito web http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm

selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Il trattamento, quindi, si concretizza in ogni tipo di operazione svolta su dati altrui, senza rilevare né il genere di operazione svolta, né il tipo di ausilio utilizzato per compierla. Tale genericità, voluta dal legislatore, permette un'applicazione estremamente ampia della disciplina, adattabile alle varie fattispecie che si potrebbero venire a creare nel corso del tempo.

Secondo l'art. 7 del D.lgs. 196/2003 l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile, laddove per interessato debba intendersi indiscriminatamente sia la persona fisica che giuridica, l'ente o l'associazione.

Il Dlgs. 196/2003 approfondisce poi i ***diritti dell'interessato***. Egli , infatti, possiede in primo luogo il diritto di conoscere le finalità e le modalità con cui verranno usati i propri dati, in secondo luogo di richiederne la cancellazione o la trasformazione dei medesimi in dati anonimi e può, altresì, opporsi al trattamento per invio di materiale pubblicitario. Ha diritto inoltre di richiedere l'interruzione del trattamento sui dati sensibili che comporta l'interruzione di tutte le operazioni che rientrano nell'art. 4 primo comma lettera "a" del decreto legislativo 196/2003.

Inoltre, l'accesso da parte dell'interessato ai dati deve essere facilitato anche per mezzo di software informatico mentre la tempista di risposta deve essere conclusa in tempi brevi.

I dati richiesti possono essere comunicati oralmente o visualizzati tramite mezzo informatico, e qualora richiesto, è possibile stamparli su supporti cartacei.

Infine, è possibile anche consegnare una copia dell'atto ove la richiesta del richiedente risulti difficoltosa.

In questo contesto, anche le Pubbliche Amministrazioni possono essere titolari del trattamento di dati personali, e come tutti i titolari sono tenute a rispettare la normativa.

Il trattamento nelle Pubbliche Amministrazioni non è da sottovalutare, infatti nella stesura del testo normativo esistono parti dedicate a questo trattamento. La ragione per cui si è sentita l'esigenza di una disciplina differente per la pubblica amministrazione dipende dal fatto di trovare un punto di equilibrio tra la protezione dei dati sensibili dei soggetti e l'esigenza della pubblica amministrazione di trattare i dati per finalità e utilità pubbliche. Occorre sicuramente considerare quanto rilevante sia, specie in particolari circostanze, privilegiare l'interesse collettivo a discapito dell'interesse dell'individuo.

Nei capitoli relativi al trattamento nell'ambito di una Pubblica Amministrazione viene prevista l'essenzialità e la necessità di effettuare trattamenti per lo svolgimento delle funzioni istituzionali: il D. lgs. 196/2003, tenendo conto dei limiti imposti dalla legge, non ha

potuto riservare il medesimo trattamento nel settore pubblico rispetto al settore privato.

Molti sono stati, infatti, i casi d'inosservanza della normativa sulla privacy nelle pubbliche amministrazioni già nel 2002, orientando in questo modo l'opera successiva di legislazione.

Ad esempio, il Consiglio Nazionale delle ricerche, è stato condannato per una cifra pari ad oltre €13.400, aveva installato, per fini di sicurezza telecamere a circuito chiuso senza avvisare il pubblico e i dipendenti attraverso appositi cartelli e avvisi.

Le sanzioni amministrative sono state adeguate alla nuova unità monetaria e ponderate, in rispetto alla gravità delle violazioni e all'efficacia della sanzione. Al legislatore, è parso quindi opportuno modificare le sanzioni, in quanto nella struttura normativa precedente alcune violazioni erano particolarmente esigue e si sono manifestate del tutto senza potere deterrente, specie se combinate a carico di titolari di consolidate condizioni economiche. A ciò, si è aggiunta anche l'evidenza per cui alcune sanzioni risultavano estremamente ridotte rispetto ad altre sanzioni pecuniarie stabilitie nello stesso ordinamento.

Per quanto concerne le sanzioni amministrative nelle pubbliche amministrazioni, è stata presunta una sanzione accessoria, costituita dalla pubblicazione dell'ordinanza del Garante.

Il trattamento illecito di dati personali riguarda tutte le inosservanze delle prescrizioni relative ai trattamenti effettuati da soggetti pubblici in relazione a dati diversi da quelli sensibili e giudiziari e alla

presentazione del consenso. L'inosservanza delle disposizioni riguardanti le materie sopra menzionate è punita con la reclusione da sei a diciotto mesi se deriva nocumento dal trattamento illecito dei dati personali, mentre per la diffusione e comunicazione con la reclusione da sei a ventiquattro mesi; inoltre sono puniti con la reclusione tutti i trattamenti che violino le disposizioni in merito da cui ne derivino rischi specifici (per dati diversi da quelli sensibili, come la diffusione di dati giudiziari) siano essi di natura pubblica o privata, inerenti anche il divieto di comunicazione e diffusione, e il divieto al trasferimento all'estero. Salvo che il fatto costituisca reato più grave, chiunque, al fine di trarne per sé o per terzi profitti, o recare danni a terzi, è punibile con la reclusione da uno a tre anni.

Lo *spamming*, ovvero l'invio di grandi quantità di messaggi indesiderati generalmente commerciali, rischia di essere sanzionato con la reclusione, se entro un tempo stabilito non vengano fornite le informazioni su modalità e finalità del trattamento dei dati acquisiti. Qualora le suddette informazioni non vengano fornite, l'autorità garante stabilirò le sanzioni penali.

Il fenomeno dello *spamming* si era diffuso ampiamente anche nel mondo della telefonia mobile, attraverso l'iniziativa di SMS commerciali indesiderati. Nel 2003, lo *spamming* nella telefonia mobile, è stato così oggetto di attenzione da parte del Garante, che ha raccolto l'istanza di un utente che aveva esposto denuncia verso una società di telefonia mobile a causa della ricezione continua di SMS promozionali, sebbene non avesse prestato mai il suo consenso. Alla società in questione è stata chiesta la sospensione

dell'invio degli SMS pubblicitari con richiesta di pagamento delle spese di ricorso pari €250 da corrispondere direttamente all'utente.

Un altro illecito penale è rappresentato dalla falsità nelle dichiarazioni e notificazioni al Garante, disciplinato dall'art.168, D. lgs. 196/2003: chiunque dichiari il falso nelle notificazioni dei trattamenti o presenti informazioni non veritiere in risposta a richieste del garante in fase di controllo, è punito con la reclusione da sei mesi a tre anni. Sono soggetti a sanzioni tutti coloro che trattano dati personali in violazione delle norme, sia il titolare che il responsabile del trattamento. Tuttavia tra sanzioni penali e pecuniarie viene data la possibilità all'autore del reato di porre rimedio entro un lasso di tempo ben determinato, a seguito dell'adozione delle misure indicate espressamente dallo stesso Garante.

1.2 Tipologie di dati personali

1.2.1 Dati sensibili

Il quadro normativo italiano ha dedicato particolare attenzione ai dati sensibili, dati che riguardano la sfera più intima e delicata delle persone, distinguendoli dai dati comuni.

L'art. 4 primo comma, lettera d) del Dlgs. 196/2003 definisce i dati sensibili come dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati

personali idonei a rivelare lo stato di salute e la vita sessuale dell'individuo.

Queste informazioni sono considerate, per la loro particolare caratteristica di fornire indicazioni strettamente legate alla persona, dati ad alto livello di riservatezza e, pertanto, ritenuti meritevoli di una tutela particolarmente rigida in relazione al fatto che potrebbero essere utilizzati in modo scorretto producendo discriminazioni fra gli individui.

Il legislatore ha voluto quindi assicurare una maggiore trasparenza sulle finalità e sulle modalità del trattamento, nonché un controllo più accurato sulla gestione di queste informazioni.

La definizione di dato sensibile è una definizione molto ampia, che rende obiettivamente difficile stabilire se un dato personale rientri o meno in questa categoria.

Se da un lato vi sono dati che certamente si possono ritenere sensibili in ogni situazione, come ad esempio una cartella clinica o un referto idoneo a rilevare lo stato di salute di un individuo, vi sono altri tipi di dati che si possono ritenere sensibili solo in relazione al contesto effettivo nel quale vengono trattati.

Ad esempio, una foto è considerata a tutti gli effetti un dato personale, infatti dal soggetto della fotografia si può risalire all'origine razziale, alle preferenze politiche, religiose, sindacali e così via; ciò posto, risulta evidente che non sia il dato di per sé a essere o meno sensibile, ma la finalità con la quale il dato verrà trattato.

Le regole di riservatezza sino a questo momento esposte, possono senz'altro essere fatte valere nei confronti di ogni persona. Tuttavia il legislatore ha voluto disciplinare in maniera più specifica il trattamento dei dati da parte delle Pubbliche Amministrazioni, ponendo regole che da un lato favoriscano la tutela dei titolari dei dati e dall'altro l'accesso di terzi a determinate informazioni in talune situazioni ritenute meritevoli di tutela.

L'articolo **60 del Dlg.196/2003** permette il trattamento dei dati idonei a rilevare lo stato di salute o la vita sessuale dei titolari, solo nel caso in cui la richiesta sia resa necessaria per fare valere un proprio diritto di rango almeno pari a quello dell'interessato; questo tipo di operazione viene definita "bilanciamento" e deve sempre essere effettuata prima di concedere l'accesso a determinati tipi di dati. Il bilanciamento si ritiene però esistente di diritto nel caso in cui la situazione giuridica che si intende tutelare mediante l'accesso agli atti, riguardi un diritto della personalità o altro tipo di diritto o libertà fondamentale e inviolabile.

Ad esempio in un concorso riservato per persone portatrici di *handicap*, l'interessato può accedere ai documenti amministrativi al fine di controllare se il candidato possegga i requisiti richiesti dal regolamento.

Un altro esempio, che si può ravvisare comunemente nell'ambito sanitario, è relativo all'acquisizione di dati certamente sensibili, che spesso risultano indispensabili per eseguire al meglio i propri servizi, laddove trattare dati comuni o anonimi non consentirebbe il raggiungimento di tale obiettivo.

L'accesso ai dati sensibili, nel settore della Pubblica Amministrazione è regolato dagli articoli 22 e 24 della legge 241/1990[7].

In sintesi gli interessati hanno diritto di poter prendere visione dei propri dati o estrarne una copia solo laddove l'interesse all'accesso sia diretto, concreto e attuale, e corrisponda ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso.

Tutti i documenti amministrativi sono accessibili tranne quelli previsti dall'art. 24, comma 1,2,3,5,6 che fanno riferimento a documenti coperti dal segreto di Stato, procedimenti tributari, all'attività della Pubblica Amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e programmazione e procedimenti selettivi nei confronti di documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi.

Ad esempio l'imprenditore a cui viene negato il permesso di costruire un edificio, ha senz'altro diritto di accedere agli atti amministrativi al fine di comprendere, nell'immediatezza, il motivo per cui gli è stato negato il consenso.

Le regole generali per il trattamento dei dati del D.lgs. 196/2003[8] espone in maniera chiara come esso debba avvenire.

I dati personali devono essere trattati in modo lecito e secondo il principio di correttezza, devono essere esatti e se è necessario aggiornati, raccolti e registrati per scopi ben precisi e chiari, e

---

7 Sito web http://www.bosettiegatti.com/info/norme/statali/1990_0241.htm

8 Decreti legislativo 196/2003

conservati per un periodo non superiore a quello consentito per la necessità dello scopo per cui sono stati raccolti. L'interessato ha diritto a essere informato tramite ***l'informativa,*** che può essere di tipo scritta o orale. Il fine e la modalità del trattamento cui sono destinati i dati devono essere espressi chiaramente e se il conferimento dati è di tipo facoltativo o obbligatorio occorre predisporre le eventuali conseguenze di un rifiuto. Inoltre l'interessato ha diritto di essere a conoscenza delle categorie di soggetti a cui i dati andranno in conferimento.

Gli estremi identificati del titolare o del responsabile, se è stato designato, devono essere reperibili all'interessato tramite appositi mezzi di cui esso deve esserne messo a conoscenza.

La cessazione del trattamento dei dati, che avvenga per un qualsiasi motivo, prevede che i dati siano distrutti o ceduti a terzi solo se il trattamento è compatibile con gli scopi per cui sono stati raccolti o ceduti ad altro titolare per scopi storici e scientifici in conformità alla legge, e infine conservati per fini esclusivamente personali e non destinati alla comunicazione o diffusione.

Il titolare che intende trattare dati sensibili deve notificare al garante il trattamento cui intende procedere solo se riguardano dati genetici, biometrici, dati idonei a rilevare lo stato di salute e la vita sessuale, malattie mentali, servizi sanitari per via telematica e così via.

La notificazione del trattamento deve essere presentata una sola volta al garante, a prescindere dal numero di operazioni e dalla durata del trattamento. La notificazione è valida se è trasmessa per via telematica utilizzando un modello messo a disposizione dal

garante, e vi è bisogno di rinnovare la notifica al garante se il trattamento dati cessa.

1.2.2 Dati Giudiziari

La definizione di dati giudiziari, è introdotta dall'art.4, primo comma, lettera e), D. Lgs.196/2003: questi sono individuati come i dati personali idonei a rilevare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato.

I dati giudiziari godono delle stesse "regole" sancite per i dati sensibili, facendo particolare distinzione anche in questo caso al trattamento di dati tra soggetti pubblici, privati ed economici.

Sono considerati dati giudiziari tutti quei provvedimenti oggetto di registrazione presso gli uffici del Casellario, con esclusione espressa di quelli che riguardano: interdizione, inabilitazione, amministrazione di sostegno, concordato fallimentare, fallimento e riabilitazione del fallito.

L'art. 21 comma 1 della stessa fonte specifica inoltre che i dati giudiziari possono essere utilizzati da soggetti pubblici solo a seguito di espressa disposizione di legge o di un provvedimento del Garante, che ne specifichino le finalità di rilevante interesse pubblico, i tipi di dati utilizzati e le operazioni eseguibili.

Tutto ciò si differenzia da quanto previsto dall'articolo 20 numero 1 sulla tutela dei "dati sensibili", per i quali è possibile il trattamento da

parte di soggetti pubblici solo nei casi previsti dalla legge, esclusa la possibilità per il Garante di autorizzarli.

Nel successivo articolo, l'art.22, titolato "*Principi applicabili al trattamento di dati sensibili e giudiziari*" viene postulato il principio che si potrebbe definire di "indispensabilità del trattamento" ovvero viene permesso il trattamento per dati sensibili e giuridici laddove l'Ente pubblico non può altrimenti compiere le proprie attività istituzionali, anche ricorrendo a dati anonimi, con particolare riferimento alle attività di pubblica sicurezza. Ad esempio, l'utilizzo dei dati custoditi nel Casellario per finalità statistiche, cadono proprio in questo ultimo caso: i dati devono essere raccolti e trattati in maniera anonima al fine di elaborare solamente informazioni di carattere generico utili per l'Ente pubblico.

Vengono anche affrontate tematiche relative alla salvaguardia e alla sicurezza dei dati. Essi infatti devono essere contenuti nel Casellario giudiziale in forma criptata e devono essere accessibili anche senza essere ricondotti ai soggetti ai quali si riferiscono. Per essere abbinati a dati anagrafici completi, occorre infatti una richiesta motivata con l'assunzione di responsabilità individuale di tale operazione. Tutto ciò al fine di tutelare le informazioni giudiziarie per evitare diffusioni non autorizzare e fughe di notizie talvolta pericolose e compromettenti, ad esempio si pensi alle indagini ancora in corso.

1.3 Il Garante e i suoi compiti

1.3.1 Nascita dell'Autorità Garante

Dopo l'emanazione della legge sulla privacy, la 675/96, nacque l'esigenza di creare un organo collegiale imparziale e con una propria soggettività giuridica al fine di avere un ente che garantisse la supervisione della materia di protezione dei dati personali nel nostro paese.

L'autorità garante fu creata dal parlamento nel 1997 non solo con lo scopo di avere un organo che supervisionasse la legge, ma anche con l'obiettivo che rispondesse alle esigenze di chiarimenti della società in merito alla materia di protezione dei dati personali.

Uno dei compiti più difficili per il garante è quello di comunicare l'esattezza della normativa alla collettività.

Per svolgere al meglio la comunicazione all'esterno questi si avvale di bollettini che raccolgono provvedimenti, risposte ai quesiti dei media e degli organi di stampa che si pongono come obiettivo la corretta divulgazione attraverso le proprie testate giornalistiche degli approfondimenti inviati dal garante settimanalmente.

Infine, per ottimizzare la promozione informativa, è stato realizzato il sito web del garante[9], anch'esso aggiornato periodicamente.

---

9 Sito web http://www.garanteprivacy.it/

L’autorità garante ha sede in Roma, ove vengono svolte le riunioni, le quali possono essere tenute anche in videoconferenza.

Essendo un organo amministrativo indipendente, il Garante ha una propria soggettività giuridica ed esercita il suo potere di vigilanza in materia della privacy.

Il mandato dei membri del garante dura quattro anni. Decorso questo lasso di tempo il Parlamento provvede all’elezione di un nuovo organo collegiale. Attualmente Francesco Pizzetti è il Presidente, Giuseppe Chiaravalloti è il Vice Presidente , Giuseppe Fortunato, Mauro Paissan, sono componenti, mentre il Dott. Buttarelli è il segretario generale.

Il presidente raffigura il Garante, e viene eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età.

I membri del collegio non possono esercitare attività professionali o di consulenza, né essere amministratori di enti pubblici o privati, né ricoprire cariche elettive, al fine di garantire una totale indipendenza.

1.3.2 Compiti del Garante

Il Garante con l'entrata in vigore della 675/1996 ha dovuto fare fronte a molti interventi, soprattutto in situazioni in cui la normativa della *privacy* va ad impattare casi particolari che con il diffondersi delle

tecnologie, cresciute in modo esponenziale, hanno dato origine a possibili vuoti normativi. Di conseguenza anche l'autorità garante ha dovuto evolversi per continuare a far sì che la normativa venisse rispettata.

Si pensi ad esempio alle segnalazioni, ai reclami, alle ispezioni e ai controlli, alle autorizzazioni generali ed individuali per il trattamento di dati sensibili, alla creazione del registro generale dei trattamento in cui sono archiviate le notifiche, all'organizzazione e al funzionamento dell'ufficio, alla predisposizione di un proprio codice etico, ai rapporti con i media, ai bollettini volti alla divulgazione degli aspetti trattati dall'autorità e altro.

I compiti del garante vengono definiti nel ***art. 154 del D. lgs. 196/2003.***

Gli adempimenti principali che permettono al garante e ai terzi di conoscere se, perché e come una determinata azienda o ente gestisca dati sensibili sono: la notificazione all'autorità garante, l'informativa all'interessato, la raccolta dei consensi, la suddivisione dei compiti con l'attribuzione delle relative responsabilità all'interno delle organizzazione del titolare e l'adozione di determinate misure di sicurezza.

La notificazione è una comunicazione ufficiale che il titolare del trattamento deve inviare per via telematica al Garante, con la quale gli si comunica l'esistenza di un'attività di raccolta e utilizzazione di dati personali e informazioni sul tipo di trattamento svolto.

Essa deve essere inviata al Garante qualora il titolare effettui il trattamento di: dati biometrici o genetici, quando il dato rileva la posizione geografica di persone od oggetti mediante mezzi di comunicazione elettronica, dati che rilevano la vita sessuale e lo stato di salute di un soggetto, come in caso di prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazioni di malattie mentali, infettive e diffusive, coma la sieropositività, il trapianto di organi e tessuti ed infine il monitoraggio della spesa sanitaria.

Occorre notificare anche i dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti.

E ancora dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie, dati registrati in apposite banche dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti e infine dati concernenti l'ubicazione di persone o oggetti mediante una rete di comunicazione elettronica.

Questo ultimo tipo di raccolta di dati, è ormai possibile grazie alle tecniche che consentono di individuare la localizzazione geografica degli utenti di telefonia mobile. Un altro esempio deriva dalla possibilità di rintracciare l'acquirente di un prodotto a cui sia stata

applicata la cosiddetta “etichetta intelligente”, ancora in fase di sperimentazione, che consentirebbe, attraverso un microchip applicato a un qualsiasi bene, la possibilità di verificare i movimenti dei singoli articoli in vendita.

Questo dispositivo comporterebbe anche dei rischi per la *privacy* delle persone, poiché tiene monitorato per ogni acquirente il tipo di acquisto nei casi in cui il microchip è stato inserito. Una forma simile di controllo si verifica abitualmente con i dati registrati per la “spesa automatica” e attraverso le “carte fedeltà”.

Grazie a quest’ultime è possibile conoscere gli acquisti collegati alla carta e di collegarli quindi con l’anagrafe completa del possessore della carta. Con la “spesa automatica”, progetto sviluppato da note catene della grande distribuzione, è anche possibile tracciare l’ordine con cui un utente compra un bene, informazione utile per finalità di marketing.

Tracciare gli acquisti di una persona aiuta a definire il profilo di essa e probabilmente a ricostruire informazioni sensibili che vanno anch’esse, quindi, trattate e tutelate.

Ai sensi dell’art.38, primo comma , D. lgs.196/2003, la notificazione deve essere presentata anche una sola volta, anteriormente all’inizio del trattamento, indipendentemente dalla durata sua durata e dalla numerosità delle operazioni e può riguardare una o più finalità correlate. Una nuova notificazione è necessaria soltanto qualora vi sia cessazione del trattamento o se si assista ad una variazione di uno o più elementi, da indicare nella notificazione stessa.

L'informativa è la comunicazione con la quale il titolare del trattamento informa l'interessato del trattamento svolto, e può essere tipo orale o scritta. Il titolare deve illustrare all'interessato la finalità e modalità del trattamento dati, l'ambito di comunicazione e diffusione dei dati, eventuali conseguenze di un rifiuto del conferimento, eventuale trasferimento all'estero dei dati, i diritti dell'interessato, indicazioni del titolare, l'indicazione del Responsabile individuato o di quello designato per l'esercizio dei diritti dell'interessato, l'indicazione degli Incaricati che compiono le operazioni di trattamento. L'informativa va resa al responsabile al momento della raccolta dei suoi dati.

Per raccolta di consensi sin intende che, non si può effettuare un trattamento dati senza il consenso del titolare, e deve essere esplicito, libero e documentato per iscritto. Con il consenso l'interessato esprime l'autorizzazione in senso generale al trattamento dei suoi dati. La mancanza del consenso comporta sanzioni penali e amministrative, ferma restando la responsabilità civile del Titolare in caso di accertamento del danno derivante da illecito trattamento. L'art. 24 del decreto legislativo 196/2003 raccoglie i casi in cui non vi è bisogno di chiedere il consenso per il trattamento.

Il titolare può dare il proprio consenso sul trattamento discriminando alcune operazioni di trattamento, escludendone altre seppur facendo parte dello stesso trattamento. Ad esempio, il consenso può essere prestato solo per la registrazione dei dati, ma non per la loro elaborazione o per il loro raffronto con altri dati.

La tutela alla riservatezza non si delimita solo al rispetto dei principi di correttezza e liceità delle singole operazioni del trattamento eseguite

dai differenti titolari , ma deve estendersi sino a comprendere sistemi tecnici, organizzativi, logistici che consentano una effettiva e concreta protezione della sfera privata dell'interessato.

Assume notevole importanza, nel complesso introdotto dalla normativa, la tutela dei dati personali non che la sicurezza delle operazioni di trattamento che deve essere garantita di pari passo con l'evoluzione tecnologica raggiunta nella consapevolezza che siamo in presenza di una sempre maggiore proliferazione dei rischi a cui i dati personali sono quotidianamente sottoposti. La crescita esponenziale di internet e l'evoluzione di mezzi tecnologici sofisticati, hanno fatto sì che la trasmissione dei dati possa avvenire senza alcuna limitazione territoriale mettendo a rischio la loro effettivamente sicura archiviazione.

I nuovi mezzi di comunicazione legati alla rete internet sono quindi molto rischiosi, in quanto permettono l'interferenza da parti di terzi in mancanza di precise procedure ed aggiornati criteri di sicurezza.

L'adozione di idonee misure di sicurezza è strettamente correlata con la riduzione dei costi, che il titolare dovrebbe sostenere al verificarsi dell'alterazione o della divulgazione di dati personali, spesso di natura sensibile. Deve, pertanto, svilupparsi una maggiore conoscenza della sicurezza ed una sensibilizzazione al trattamento attraverso la pianificazione di un budget di spesa dedicato agli aggiornamenti e alla configurazione di sistemi informatici idonei. L'adozione di aggiornate misure di sicurezza deve essere garantita dal momento della pianificazione di un trattamento e sin dalla sua concreta esecuzione. Il legislatore italiano ha individuato alcune regole di base considerate minime e definite nel D. Lgs.196/2003.

Il Garante deve controllare che i trattamenti dei dati sensibili vengano effettuati nel rispetto della disciplina e in conformità alla notificazione anche in caso di cessazione dei trattamenti.

Deve esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o alle associazioni che li rappresentino. Questa attività ha luogo in quanto il Garante riceve reclami da singoli privati, da associazioni di consumatori che avvisano il Garante della non osservanza della normativa.

Deve prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento lecito qualora vengano segnalati reclami. Deve vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco, ovvero emettere blocchi correttivi.

Segnalare a parlamento e governo l'opportunità di procedere con interventi normativi per fare si che i diritti di libertà, dignità, riservatezza, protezione dei dati vengano rispettati.

Deve inoltre esprimere pareri qualora vengano richiesti.

Ma soprattutto deve diffondere la conoscenza tra l'utenza della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati.

Si occupa di denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle proprie funzioni.

Tenere il registro dei trattamenti formato sulla base delle notificazioni e promuovere il codice di deontologia e buona condotta.

Annualmente il Garante è tenuto a predisporre una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che viene trasmessa al parlamento e al governo entro il 30 Aprile dell'anno successivo a quello cui si riferisce.

Deve inoltre svolgere la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari.

In particolare, il Garante deve aggiungere ai compiti appena espressi, il dovere di modifica, di ratifica e di esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen non che alla relativa convenzione di applicazione e alle successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (*Europol*) e alle successive modificazioni, di ratifica ed esecuzione, della convenzione sull'uso dell'informatica nel settore doganale.

Deve inoltre attenersi al regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"***Eurodac***" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino.

Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altre autorità, prendendo

parte alla discussione di argomenti di comune interesse ove può richiedere, altresì, la collaborazione di personale specializzato addetto.

Un aspetto molto importante dell'attività dell'autorità garante è il rilascio delle autorizzazioni per il trattamento dei dati sensibili e giudiziari, nonché al trasferimento dei dati all'estero. Il compito correlato al rilascio delle autorizzazioni consiste nel valutare se la richiesta fatta dal responsabile in merito a un trattamento dati sia sia idonea o meno. Le autorizzazioni possono essere di tipo individuali, rilasciate al singolo titolare, o di tipo collettivo, rilasciate dalle ***autorizzazioni collettive.***

Le autorizzazioni collettive nascono con la finalità di alleggerire la burocrazia e l'organizzazione delle attività per il garante.

Le autorizzazioni generali permettono ad un titolare di non richiedere il consenso per un determinato trattamento, sempre che il trattamento medesimo rispetti i limiti e le prescrizioni contenute nelle autorizzazioni collettive. Le richieste di autorizzazione individuali posso essere fatte tramite la modulistica messa a disposizione dal garante con gli stessi mezzi messi a disposizione per le notifiche.

La funzione del Garante si esplica attraverso interventi di carattere inibitorio, cautelare o sanzionatorio finalizzati alla risoluzione dei conflitti fra l'interessato ed il titolare del trattamento. Questa funzione può essere attivata d'ufficio o a seguito di una segnalazione o di un reclamo. Questi poteri sono perciò indirizzati alla prevenzione ed alla repressione di illeciti in materia e possono essere esercitati tanto nei

confronti di un intero trattamento quanto in riferimento ad una sua parte soltanto.

L'art.157 del D.Lgs 196/2003 stabilisce che il Garante possa richiedere al titolare, al responsabile, all'interessato o anche a soggetti terzi di fornire informazioni e di esibire documenti. E' questa una prima modalità di verifica sulla corretta applicazione della legge sulla privacy, volta ad acquisire primi elementi di valutazione che possono essere sufficienti allo scopo di indurre il garante a procedere verso controlli più specifici e circostanziati, che si esplicano in accertamenti ed ispezioni, nonché ad accessi a banche dati. Viceversa, è possibile che, a seguito di accertamenti, il garante possa richiedere l'esibizione di documentazione o il rilascio di altre informazioni.

L’accesso alle banche dati, le ispezioni e le verifiche possono essere eseguite informando il titolare o il responsabile o, se è assente o non nominato, anche gli incaricati del trattamento. Il personale d'Ufficio deve essere munito di documento di riconoscimento e può essere assistito da consulenti. Possono essere estratte copie di documenti, anche a campioni e su supporto informatico o per via telematica. Al termine delle operazioni di accertamenti sarà redatto un verbale riportante i risultati dell'ispezione e anche eventuali dichiarazioni dei presenti. Una volta terminato l'accertamento, il Garante rileva la violazione della normativa, e se sussistono elementi probatori del trattamento illecito e non conforme al codice, indica al responsabile o al titolare le misure modificative o integrative a correzione, e ne verifica l'adozione. Se l'accertamento è stato richiesto dall'interessato, il garante provvederà a comunicargli l'esito dell'accertamento.

Il codice etico del Garante nasce con il fine di dare un esempio a quei settori nei quali viene promossa la disciplina. L'obiettivo del codice etico è quello di definire una serie di linee guide di comportamento che i soggetti che compongono l'ufficio del garante devono eseguire nello svolgimento della loro attività. Questi principi si concretizzano nei doveri di lealtà, di imparzialità, di diligenza e di operosità. Coloro che operano per l'Autorithy devono svolgere i propri compiti tenendo ben presente i doveri di indipendenza e di rispetto degli obblighi di riservatezza e segretezza delle informazioni conosciute nell'ambito delle proprie mansioni e, non ultimi, i principi di imparzialità e di trasparenza delle proprie mansioni e nelle attività di amministrative.

Devono essere mantenute la riservatezza assoluta nei confronti di tutte le informazioni acquisite nell'espletamento delle proprie mansioni ed anche successivamente alla cessazione del periodo di servizio presso l'ufficio. I dipendenti dell'Ufficio devono essere cordiali, efficienti e disponibili, onde manifestare il proprio impegno a favore della salvaguardia della privacy delle persone. Analogo deve essere il comportamento nei confronti dei colleghi e collaboratori e dipendenti dell'ufficio.

Per dovere di imparzialità si intende che non siano ammessi favoritismi, situazioni privilegiate e condizionamenti.

Nel codice etico è affrontato anche il tema del conflitto di interesse che potrebbe sorgere in riferimento ad attività precedenti svolte dal componente dell'Ufficio: il dipendente deve astenersi dal partecipare, per almeno due anni, dal trattare questioni che sono di competenza del Garante e che coinvolgono propri precedenti soci in affari o precedenti datori di lavoro. Alla base del codice etico stanno i principi

di condotta che perseguono il fine di raggiungere la correttezza professionale, inibendo qualsiasi atteggiamento, azione o dichiarazione che rischi di sminuire il ruolo di giudice imparziale. Questa specifica regola di condotta è evidenziata con particolare riferimento ai rapporti con gli organi di stampa.

Il codice etico, può, infine, essere aggiornato sulla base dell'esperienza acquisita nel corso del tempo, senza porre una scadenza sistematica ad una sua messa in discussione.

Capitolo secondo

2.1. Problematiche correlate all'uso dei mezzi informatici da parte dei lavoratori

2.1.1 Introduzione alle problematiche

In questo capitolo si analizzeranno i problemi legati allo sviluppo delle tecnologie informatiche con riferimento all'ambito aziendale.

La nascita di internet a livello mondiale ha fatto si che ci si ponessero diversi quesiti in merito alla libera circolazione dell'informazione in rete.

Quotidianamente le informazioni vengono monitorate attraverso vari mezzi telematici. Si pensi alla carta di credito che raccoglie informazioni sulle preferenze di acquisto degli utenti, o ai *cookies* che si auto installano sul disco fisso dei PC al fine di raccogliere informazioni che saranno elaborate dalle aziende per creare pubblicità mirate per l'utente attraverso *software* appositi.

L'avvento di internet ha abbattuto le barriere geografiche e ha reso molto semplice venire in contatto con dati senza discernimento fra soggetti pubblici, privati, attività economiche, enti o organizzazioni private o pubbliche.

La circolazione di questi dati non era inizialmente disciplinata da alcuna regola, e quindi non veniva assicurata nessuna tutela al diritto

alla riservatezza e all'integrità dei dati. Per questo motivo è nata l'esigenza di emanare una normativa per regolare tali diritti in rispetto della *privacy*.

La nascita di tecnologie sempre più sofisticate ha fatto sì che le aziende usassero queste risorse al fine di controllare i dipendenti all'interno delle aziende. Il controllo può essere di tipo visivo, come le telecamere, o "invisibile", come ad esempio specifici programmi installati nei personal computer al fine di tracciare la navigazione del dipendente.

Alcune motivazioni per cui un datore di lavoro traccia e/o videosorveglia un dipendente possono essere le seguenti:

- Uso delle risorse aziendali a scopo personale sottraendo ore di lavoro per fini personali;

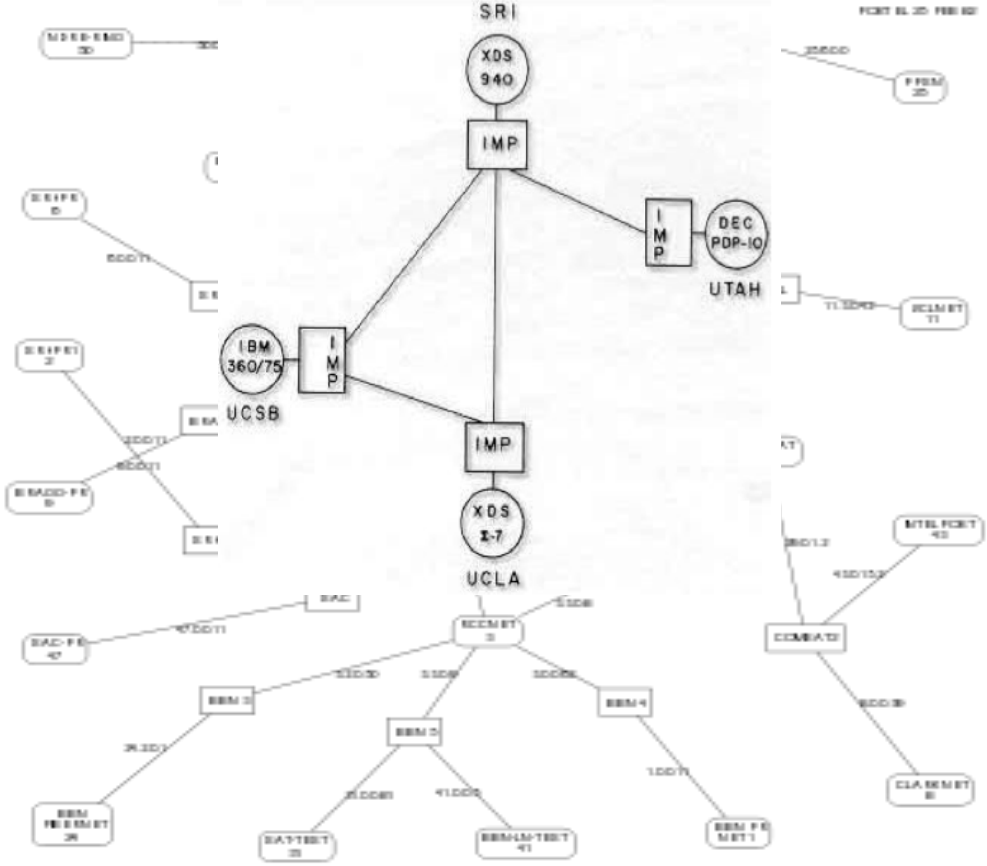
- Fuga di notizie in merito alle strategie elaborate dalle aziende al fine di perseguire uno scopo economico (spionaggio aziendale);

- Uso delle risorse di internet per scaricare musica, video, materiali pornografici e più generalmente files coperti dal diritto d'autore o comunque illeciti, come il materiale pedo-pornografico.

E' così che i dipendenti si trovano ad essere controllati costantemente senza, molto spesso, esserne al corrente.

A tale proposito l'autorità garante ha stabilito che **"è illecito spiare il contenuto della navigazione di internet del dipendente."**

Dettagli che verranno affrontati nei capitoli successivi.



2.1.2 Cenni alla nascita di internet

Internet nasce da un progetto statunitense chiamato Arpanet[10], quando nel 1969 furono collegati per la prima volta quattro computer in rete. Arpanet permetteva una connessione di tipo client-server, e non permetteva un collegamento diretto di tipo host to host.

Con la nascita della tecnica della ***commutazione di pacchetto*** Arpanet espanse i propri nodi oltre oceano.

Figura 1: *Composizione iniziale di Arpanet 1969* [11].

---

10 Sito web http://it.wikipedia.org/wiki/Internet

11 Sito web http://www.dariobonacina.net/Internetstory.pdf

Figura 2: *Arpanet nel 1982* [12].

La tecnica della ***commutazione di pacchetto*** permette di avere accessi multipli ripartiti nel tempo ed è utilizzata per accedere a un canale condiviso tra più utenti. I pacchetti vengono processati velocemente senza bloccare la comunicazione. Questo concetto ha trovato un'ampia diffusione facendo sorgere le prime reti, come quella universitaria di JANET e la rete pubblica americana CompuServe, una società commerciale che consentiva a piccole imprese ed individui di poter accedere alla condivisione delle risorse del computer, cosa che in seguito diventerà l'accesso ad Internet.

I primi servizi offerti da questo tipo rete erano:

- ***E-mail***

- ***FTP (File Transfer Protocol)***

- ***HTTP (HyperText Trasnfer Protocol)***

La proliferazione di diverse reti ha fatto sorgere il problema di come riuscire a collegare reti di tipo diverso tra di loro. ***Robert Kahn*** e ***Vinton Cerf*** elaborarono una tecnica che mascherava la diversità delle reti al fine di riuscire a collegare più reti tra loro indipendentemente dalla loro natura.

Dal 1981 le specifiche furono concluse, pubblicate ed adottate: nel 1982 le connessioni ARPANET al di fuori degli USA furono convertite e fu utilizzato il nuovo protocollo ***TCP/IP (Transmission Control Protocol / Internet Protocol)***.

---

[12] Sito web http://it.wikipedia.org/wiki/Internet

Il protocollo ***TCP/IP*** serve per trasmettere i dati in modo affidabile tra reti di computer. Una rete di computer altro non è che un insieme di calcolatori interconnessi tra di loro, sia a livello hardware sia a livello software con il fine di avere una condivisione di informazioni tra più computer.

Nel 1991 ***Tim Berners Lee*** definì l'***HyperText Transfer Protocol*** come sistema ipertestuale che permette un lettura dei documenti non sequenziale ma ipertestuale, cioè i documenti venivano organizzati in e messi in relazione l'uno con l'altro tramite alcune parole chiave che danno vita ad appositi collegamenti. Si può pensare ad un ipertesto come ad una rete in cui i documenti rappresentano i nodi mentre le parole chiave sono gli archi di collegamento tra i nodi.

Nascono così i primi browser (Napster e Internet Explorer) e di conseguenza prende vita il World Wide Web.

Rendendo la commutazione di pacchetti e il linguaggio di scrittura di ipertesti gratuiti, il WWW ha avuto una crescita esponenziale, in quanto l'uso di questa risorsa si è allargata e diffusa anche in ambito pubblico e non solo per fini scientifici, militari e universitari.

Sempre all'inizio degli anni 90 le regole di accesso a NSTnet sono state modificate, consentendo l'ingresso in rete alle aziende per fini commerciali. Questo consenso ha apportato alla rete grandi cambiamenti, nonché una grande crescita.

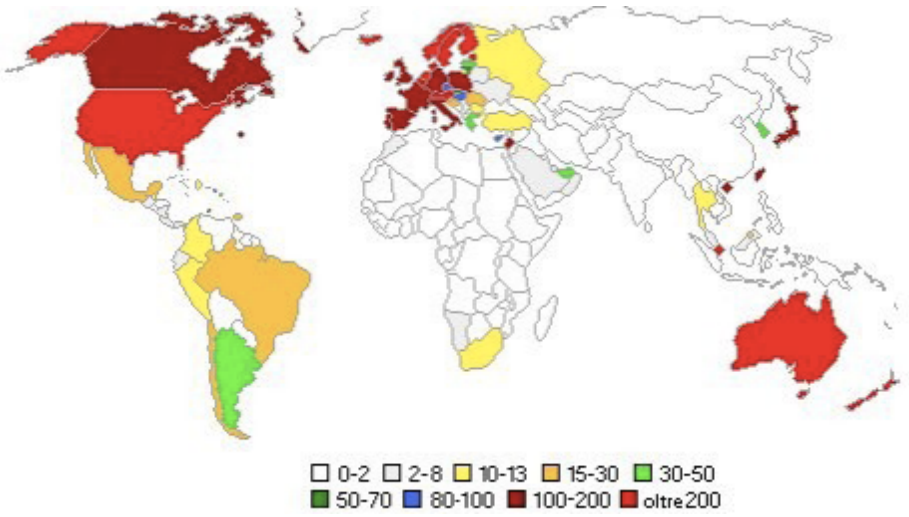


Figura 3: *numero di host per 1000 abitanti*[13].

Nasce così la necessità per le aziende di pubblicizzare i propri prodotti su internet, cercando di avvicinarsi sempre di più alle esigenze di acquisto del consumatore. Per ottenere sempre più informazioni sul consumatore le aziende hanno bisogno di conoscere preferenze, stili di vita, hobby e magari anche reddito medio dei propri utenti.

Le raccolte di questi dati venivano fatte tramite soluzioni informatiche spesso subdole, al posto dei tradizionali questionari o telefonate a campione, quasi sempre senza possedere il consenso dell'interessato.

E' quindi sorta spontanea l'esigenza di tutelare la sfera privata dei soggetti anche in rete e di creare una normativa che disciplini con maggiore rigore il diritto alla riservatezza.

---

[13] Fonte *www.gandalf.it*

Questo è il primo punto di una serie di problematiche legate ad internet. La rete nasce per natura libera, in essa circolano milioni di dati di ogni tipo. L'informazione può essere di tipo audio, video o testuale, non essendoci un supervisore che controlla la rete, la responsabilità dei contenuti su internet ricade sui provider.

Un provider è un organizzazione che offre agli utenti (residenziali o imprese) servizi generici inerenti la rete internet: i principali servizi sono rappresentati dalla fornitura dell'accesso ad Internet con la messa a disposizione di un server su cui implementare il proprio sito web e la possibilità di generare, spesso gratuitamente, un indirizzo di posta elettronica.

Nascono quindi diversi tipi provider, come i prestatori di servizi di memorizzazione temporaneo e i prestatori di memorizzazione di informazione. Questo contesto è stato disciplinato dalla direttiva 31/2000 CE.

Un altro aspetto cruciale che analizzeremo è l'uso sempre più frequente della posta elettronica.

La posta elettronica ha semplificato ma soprattutto velocizzato l'invio di materiale digitale e sempre più utenti ne fanno uso quotidianamente.

Il suo utilizzo è impiegato sia per comunicazioni formali tra utenti, sia per lo scambio di messaggi tra amici, il tutto gestito tramite server tecnicamente complessi ma in modo semplice e veloce dal lato utente.

La diffusione tra le persone dell'utilizzo dell'e-mail è cresciuta in modo esponenziale per svariati motivi:

- Non è necessaria una connessione veloce.
- Le e-mail arrivano a destinazione anche quando l'utente non è connesso.
- - E' possibile effettuare l'invio multiplo di un messaggio a più destinatari.
- Le e-mail si possono ricevere e leggere in qualsiasi parte del mondo, in cui sia disponibile un terminale e una connessione.
- I messaggi sono recapitati in qualunque parte del mondo.
- Le tempistiche di invio e di ricezione sono estremamente ridotte.
- Il costo di questo servizio è minimo.
- Si posso allegare file al contenuto testuale della mail.

Molte strutture pubbliche hanno adottato questo mezzo di comunicazione. In particolare analizzeremo i settori aziendali per capire meglio quali siano state le ripercussioni in questo contesto.

2.1.3 Problemi legati all'uso di internet ed e-mail in azienda

Internet è stato introdotto nelle aziende con il fine di semplificare la comunicazione interna ed esterna dell'azienda, per migliorare e

semplificare l'interazione con il cliente, nonché migliorare la comunicazione con i dipendenti stessi.

Per comunicazione interna si intendono tutte le risorse umane e tecnologiche che vengano usate con il fine di semplificare la stessa interazione tra dipendenti e superiori. Aspetto molto importante per le società, in quanto diminuiscono le tempiste di risposta in merito a problematiche aziendali.

Si pensi ad esempio ad una società composta da oltre 300 dipendenti a cui occorre fare pervenire una comunicazione scritta. Probabilmente prima dell'introduzione di internet si avrebbe provveduto con l'invio della comunicazione attraverso i classici mezzi cartacei o la diffusione di cartelli in apposite bacheche. Se si ragiona in termini di costi, una diffusione di questo tipo comporta un onere per l'azienda stessa unito ad una perdita evidente di tempo.

Con il servizio delle e-mail è molto più facile e veloce fare pervenire comunicazioni di ogni tipo.

La comunicazione esterna, per via di questi mezzi tecnologici permette alle società di comunicare con il cliente o l'utenza in modo interattivo.

Ad esempio tutte le aziende ormai possiedono caselle email per i reclami a cui i consumatori possono rivolgersi. Un altro esempio potrebbe essere il web marketing. Aspetti tutti importanti e positivi per le società, che in questo modo selezionano meglio il target e danno vita a campagne marketing mirate alle esigenze dell'utenza, una volta

rielaborate le informazioni in proprio possesso, agevolando il percorso di vendita.

L'uso di internet ha dato luogo, quindi, ad alcune problematiche legate all'uso di questo mezzo, ed in particolare in relazione all'uso delle e-mail da parte dei dipendenti per scopi personali, nonché all'utilizzo della navigazione per scopi personali nelle ore lavorative.

L'azienda si è trovata ad affrontare il problema dell'uso improprio delle risorse aziendali da parte dei dipendenti. Per uso improprio si intende la navigazione e l'uso di e-mail per fini che esulano da quelli aziendali durante le ore di lavoro.

Per ovviare a questo problema si iniziarono ad installare programmi con il compito di tracciare la navigazione del dipendente, di rielaborare il file *log* del pc, non che di controllare i *cookies* generati all'interno dei *browser*. Un file log è un file che risiede su ogni personal computer, e ha il compito di tracciare la navigazione su internet.

Tramite un file *log* è possibile invece risalire con molta facilità ai dati sensibili del dipendente, dove abbiamo spiegato che per dati sensibili si intendono tutte quelle informazioni che fanno riferimento alla vita sessuale, all'orientamento politico, all'appartenenza religiosa di un soggetto, ognuna di esse quasi sempre ricavabile analizzando la cronologia di navigazione.

Questo problema fu oggetto di discussione in molte aziende, in quanto i datori di lavoro, prima che ci fosse una normativa che regolamentasse la problematica, presero decisioni in merito con

provvedimenti disciplinari, video sorveglianze, e nella maggiore dei casi con il licenziamento diretto del dipendente.

Un altro oggetto di discussione per cui il garante ha dovuto prendere provvedimenti è l'utilizzo delle e-mail per uso personale; anche in questo caso prima del provvedimento del garante, ci sono state molte situazioni in cui il datore di lavoro ha controllato le caselle e-mail del dipendente, senza il consenso dello stesso.

I dipendenti hanno fatto ricorso allo statuto del lavorare per tutelare i propri diritti, come il diritto alla privacy, il diritto alla riservatezza, e il diritto alla tutela del trattamento dei dati personali/sensibili.

2.2 Uso improprio di internet e posta elettronica da parte dei dipendenti: Diritti del Lavoratore

2.2.1 Cenni Storici sulla legge 300/1970

Quando si parla dello statuto dei lavoratori si fa riferimento alla legge 300 del 20 maggio del 1970 , che a sua volta fa riferimento alle norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro.

Ripercorriamo velocemente la nascita dello statuto dei lavoratori.

Nella seconda metà del novecento, quando l'Italia e altri paesi si riprendevano da uno stato post-fascista, nacque l'esigenza di regolare nuovamente i rapporti lavorativi tra dipendenti e datori di lavoro.

In un paese dove la democrazia cresceva sempre di più, e dove la Carta costituzionale[14] fu approvata con, come primo articolo, il riferimento al lavoro come punto fondamentale dell'ordinamento della Repubblica, non si potevano non mettere in evidenza le implicazioni conseguenti nel rapporto fra datore di lavoro e lavoratore dipendente.

Il movimento a favore di un maggiore riconoscimento di diritti per il lavoratore dipendente coinvolgeva inizialmente solo i partiti di sinistra e ceti interessati. In opposizione si formarono partiti che sostennero politicamente le classi padronali. Il riconoscimento di alcune norme fu

---

14 Sito web http://it.wikipedia.org/wiki/Statuto_dei_lavoratori.

un percorso lungo e travagliato, ma che ottenne diversi riconoscimenti come:

- La fissazione di limiti minimi di età per il lavoro minorile;
- La riduzione della durata della giornata lavorativa ad 11 ore per i minori ed a 12 per le donne;
- Il diritto di associazione sindacale e quello di sciopero;
- Normative antinfortunistiche e l'obbligo di forme assicurative**.**

Le lotte sindacali catturarono l'attenzione generale, ci furono sempre più occupazioni di fabbriche e lotte nelle piazze, con il fine di ottenere i diritti spettanti come il salario unico o il rispetto dei contratti.

Le classi imprenditoriali invece continuavano a ribattere che la forza lavoro non poteva prendere decisioni in merito alle strategie aziendali e politiche.

Con la nascita dello statuto i sindacati sarebbero stati da lì in poi i mediatori tra la classe lavoratrice e la classe degli imprenditori.

2.2.2 Diritti del lavoratore

L'articolo 1 dello statuto dei lavoratori decreta in particolare il diritto al rispetto della dignità del lavoratore, nel senso che il lavoratore ha diritto di avere un'opinione politica o sindacale o religiosa, e questo non può essere oggetto di discriminazione sul posto di lavoro, mentre l'art. 4 vieta l'installazione di telecamere al fine di videosorvegliare il

dipendente a distanza, in quanto vengono violati i principi fondamentali della legge sulla *privacy*.

Introduciamo questi due articoli con il fine di spiegare e ricordare i limiti con cui un datore di lavoratore può eseguire i propri controlli sull'utilizzo delle risorse aziendali.

La videosorveglianza è un mezzo di controllo che si è diffuso in molte aziende, anche per finalità probatorie.

Si premette che non tutto ciò che è tecnologicamente possibile lo sia anche in termini giuridici.

L'oggetto in discussione è il dato personale, ove per ***dato personale*** s'intende "*qualunque informazione concernente persona identificata o identificabile*". La video sorveglianza viola tramite la registrazione di immagini o flussi video, che permettono chiaramente il riconoscimento del soggetto tracciato.

Il trattamento dei dati personali con l'utilizzo di apparecchiature di video sorveglianza è disciplinato dal provvedimento generale del garante per la protezione dei dati personali, del ***29 Aprile 2004***[15]***.***

Pertanto, la videosorveglianza è lecita solo nei casi in cui gli altri mezzi di sicurezza risultino insufficienti.

L'adozione di questo mezzo deve essere considerata come scelta dettata dall'insufficienza degli altri sistemi di deterrenza, e non già come la scelta più conveniente, in termini economici e non solo.

---

15 Bollettino del Garante 24 aprile 2004.

Nel caso in cui la videosorveglianza sia necessaria e autorizzata, e adottata nei limiti stabiliti dalla legge, vi è comunque l'obbligo di informare il dipendente dell'esistenza di telecamere, e di limitare tale utilizzo solo nelle area lavorative ed evitare zone come spogliatoi, bagni, cabine docce e così via.

Va anche specificato che le videoregistrazioni possono essere conservate per un periodo non superiore ad una settimana, e i dati contenuti nelle registrazioni devono essere finalizzati all'obiettivo per cui sono stati raccolti.

A rafforzare l'art. 4 occorre citare anche l'art.3, che ha una rilevante importanza al fine di proteggere il dipendente.

L'art. 3 afferma che il datore di lavoro non può assegnare a un personale di vigilanza il compito di controllare l'attività lavorativa di un dipendente, ma può esercitare vigilanza esclusivamente sul patrimonio aziendale.

Il dipendente può esercitare il diritto della libera circolazione in ogni luogo, ma soprattutto può esercitare il diritto di poter svolgere le proprie mansioni senza essere soggetta a condizionamenti psicologici quanto al movimento o al comportamento.

La ***direttiva 95/46/CE e la convenzione n.108/1981*** sottolineano il trattamento di materiale visivo, audio per la protezione delle persone soggette al trattamento automatizzato di dati a carattere personale.

I principi di tale direttive si applicano ad ogni tipologia di materiale di tipo visivo, audiovisivo, multimediali ed alle apparecchiature utilizzate dai titolari del trattamento per identificare soggetti.

Con l'introduzione di nuovi mezzi tecnologici e internet in azienda, nasce l'esigenza di disciplinare non solo la videosorveglianza, ma anche la navigazione web, tracciabile senza consenso tramite *software* spia. Tali software sono capaci di tracciare e controllare qualsiasi attività effettuata su un personal computer, anche in questo caso senza rispettare i principi fondamentali sul trattamento dei dati sensibili, come il diritto alla riservatezza e il diritto alla *privacy*.

A tale proposito la Corte di cassazione interviene per regolare tramite la sentenza ***n. 4375/2010*** l'uso di questo software.

La ***sentenza***[16] ***n. 4375/2010*** emana che il datore di lavoro non può installare *software* spia all'insaputa del dipendente con l'obiettivo di tracciare la navigazione web dello stesso nelle ore di lavoro, a meno che non ci sia il consenso preventivo delle associazioni sindacali.

Proponiamo un caso di licenziamento di un dipendente per uso indebito di internet.

Il caso storico da cui prende spunto tale decisione [17] *riguarda un impiegato che svolgeva mansioni di addetto all'accettazione ed al banco referti di una clinica, che è stato licenziato per giusta causa, avendo effettuato accessi non autorizzati ad Internet.*

Inizialmente costui aveva richiesto alla propria azienda di bloccare e cancellare i file ed i dati temporanei derivanti dalla navigazione in siti internet, avvenuta durante sessioni di lavoro avviate con la propria password.

---

16 Sito web http://www.cortedicassazione.it/Notizie/Notizie.asp

17 Sito web http://www.unioneconsulenti.it/article.php?sid=1349

Non avendo ricevuto un riscontro positivo da parte del proprio datore di lavoro, il dipendente si era rivolto al Garante, adducendo l' illiceità del trattamento dei dati in quanto dalla directory del lavoratore risultavano informazioni particolarmente riservate quali le proprie convinzioni religiose, opinioni sindacali e tendenze sessuali, che la società non poteva acquisire senza il suo consenso informato.

Da parte sua l'impresa traeva spunto per muovere delle contestazioni al proprio dipendente circa l'illecito accesso a Internet dai computer aziendali, l'appropriazione indebita di carta per stampare i risultati della navigazione e il danneggiamento della rete aziendale per i virus informatici che si erano introdotti nel sistema: da tale contestazione era scaturito il provvedimento disciplinare del licenziamento.

Il Garante ha accolto le ragioni del dipendente, sostenendo che l'uso indebito del computer aziendale non può essere contestato attraverso il controllo dei siti internet da lui visitati, in quanto vengono ad essere menomate delle fondamentali garanzie di spessore costituzionale quale è la libertà e la segretezza delle comunicazioni, che ricevono tutela anche da parte dello Statuto dei lavoratori.

Secondo il principio di proporzionalità, canone fondamentale nell'alveo della regolamentazione della tutela dei dati personali, sarebbe stato sufficiente verificare gli avvenuti accessi a internet e la relativa tempistica di connessione, senza per questo dover necessariamente indagare sugli aspetti contenutisti dei siti internet a cui il dipendente ha avuto accesso.

La Corte di cassazione conferma l'annullamento del licenziamento del dipendente perché ha usato internet per scopi del tutto personali, ma

conclude affermando che egli può farne uso per fine personale senza un eccessivo abuso di tale risorsa.

Altre misure di controllo che sono state adottate dai datori di lavoro per controllare dipendenti che lavorano fuori sede sono: i navigatori satellitari posizionati nelle vetture aziendali o i cellulari aziendali dotati sempre di un dispositivo satellitare.

2.2.3 Il controllo e-mail in azienda e la delibera del 1 Marzo n.13 del 2007

Un altro tema su cui l'autorità garante ha dovuto esprimersi è l'uso della ***posta elettronica nelle aziende*** da parte dei dipendenti.

Anche in questo caso l'autorità garante ha dovuto disciplinare tramite la ***delibera n.13 del 1° marzo 2007*** il trattamento dei dati e i diritti e doveri del dipendente.

Sempre più dipendenti sono soggetti a controlli per via dell'utilizzo illecito nelle ore di lavoro e così come per la navigazione web, anche per le mail si può estrarre il *file log* del traffico e-mail e in più si possono leggere le mail archiviate.

In tale modo il datore di lavoro può risalire ad informazioni private del dipendente e di terzi, nonché ricostruire la vita privata del soggetto, violando così l'art.4 dello statuto dei lavoratori, e violando tutti i principi del trattamento dei dati personali.

I casi di dibattito si sono verificati quando il datore di lavoro ha fatto accesso alla posta del dipendente per recuperare informazioni utili

alla propria attività, e nel farlo è venuto a conoscenza che tale strumento viene usato anche per fini personali; molti datori di lavoro hanno preso provvedimenti disciplinari nei confronti dei lavoratori con il licenziamento. I dipendenti a loro difesa si sono appellati allo statuto dei lavoratori e hanno segnalato i vari casi al Garante in merito ai dati personali e sensibili archiviati in azienda. Le aziende tendono a conservare tali informazioni con il fine di dimostrare l'utilizzo illecito degli strumenti. Il garante in merito a queste segnalazioni ha risposto tramite la ***delibera n.13 del 1° marzo 2007***[18]

Nel provvedimento citato, il Garante fornisce alcune **indicazioni in ordine all'uso dei computer in azienda**.

L'Autorità prescrive al datore di lavoro l'obbligo di **informare il lavoratore** delle modalità di utilizzo di Internet e della posta elettronica. Vengono indicate una serie di misure tecnologiche e organizzative per evitare la possibilità, prevista solo in casi limitati, dell'analisi del contenuto della navigazione e dell'apertura di messaggi di posta elettronica contenenti dati necessari per l'attività aziendale. Il provvedimento raccomanda l'adozione di un **disciplinare interno** nel quale devono essere indicate le regole per l'uso di Internet e della posta elettronica. Il disciplinare, redatto in modo chiaro e senza formule generiche, deve essere pubblicizzato adeguatamente e sottoposto ad aggiornamento periodico.

Il dipendente deve inoltre essere messo a conoscenza delle conseguenze disciplinari alle quali va in contro se utilizza indebitamente e-mail e internet; e deve essere messo a conoscenza

---

[18] Sito web http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522

che in caso di assenza per malattia o per ferie debba essere garantita la continuità dell'attività lavorativa, con particolare attenzione all'attivazione di sistemi di risposta automatica nei casi di messaggi di posta elettronica ricevuti.

Le suddette regole servono al dipendente per conoscere i limiti di utilizzo delle risorse aziendali, e al datore di lavoro per tutelare l'utilizzo indebito di tale risorse, nonché a colmare un divario di lavoro sforzo e stipendio, nel senso che a un dipendente viene dato uno stipendio calcolato sulle prestazione offerte e alle ore di lavoro realmente eseguite, nel momento in cui egli spreca il tempo che dovrebbe dedicare al suo lavoro per fini personali può risultare un'inadempienza verso l'impegno preso conl'impresa.

E' giusto sensibilizzare il dipende con dei confini ben precisi nell'utilizzo delle risorse aziendali, ma è anche giusto sensibilizzare il datore di lavoro a rispettare la *privacy* del dipendente e tutti i dati a cui il dipendente ha accesso.

2.3 Controlli da parte del datore di lavoro

2.3.1 Il codice disciplinare

E' stato opportuno disciplinare i controlli che venivano effettuati dai datori di lavoro sull'utilizzo dei beni aziendali. A tale proposito l'autorità garante ha preso la decisione di dare delle misure a cui il datore di lavoro deve attenersi. Il provvedimento ***del 13 Marzo 2007, numero 1***, nasce dall'esigenza di rispondere a domande che erano state poste al garante, e ai vari reclami che gli erano stati inviati in merito ai confini di controllo con cui il datore di lavoro può controllare la posta elettronica del dipendente e le risorse aziendali.

Nasce così l'esigenza di scrivere un codice disciplinare con il fine di regolamentare questo aspetto diventato un problema diffuso della società odierna.

2.3.2 Il concetto di gradualità dei controlli

Per concetto di gradualità s'intende un concetto per cui il datore di lavoro deve adottare tutte le misure per evitare l'uso improprio di internet, il controllo deve essere giustificato per poter interferire nella libertà del lavoratore.

Il controllo lecito deve essere giustificato da una situazione illecita o pericolosa e devono essere attive tutte le minime misure elencate in precedenza.

Per situazione illecita si può pensare ad esempio, a un dipendente che scarica materiale pedo-pornografico dalla postazione di lavoro.

Un personal computer è identificato univocamente tramite un IP all'interno della rete.

In caso di controllo da parte dell'autorità giudiziaria sulla postazione collegata ad un determinato IP in relazione all'illecito segnalato, l'azienda può imbattersi in sanzioni amministrative, anche a seguito di un'ulteriore verifica che ne rilevi in maniera univoca l'identità del dipendente collegato a suddetta postazione. In tal caso, in un successivo momento, il responsabile univoco dell'illecito verrà perseguito penalmente dalla legge.

2.3.3 Doveri del datore di lavoro

Il principio di ***necessità*** deve essere applicato anche nei sistemi informatici e programmi informatici, per fare sì che il trattamento dei dati sensibili sia minimizzato il più possibile.

Vi deve essere anche il principio di correttezza, il dipendente deve essere messo a conoscenza del fine del trattamento dato, inoltre il trattamento deve essere effettuato per finalità bene precise e esplicite, osservando il principio di pertinenza e non eccedenza.(**art. 11, comma 1, lett. b), del Codice: par. 4 e 5*)*).

Il datore di lavoro può eseguire controlli di monitoraggio nelle aree di rischio dell'azienda nel rispetto delle norme che vigilano su tale

argomento; il trattamento dati può essere eseguito adottando misure poco invasive.

Il provvedimento del garante specifica come l'imprenditore titolare del trattamento deve fare per ridurre al minimo la possibilità che si manifestino determinate situazioni, tra le quali rientrano:

- Bloccare siti che non ritengono utili per lo scopo dell'attività produttiva dell'azienda;

- Utilizzo di filtri che oscurano siti con finalità di upload e download;

- La conservazione dei dati deve essere tenuta archiviata per periodi brevi e per scopi produttivi e di sicurezza aziendale.

Per quanto riguarda le e-mail, il datore di lavoro deve mettere a disposizione delle caselle email condivise e non personali, in modo tale da permettere l'accesso anche in caso di assenza del dipendente.

In caso di assenza programmata del dipendente, il datore di lavoro deve mettere a disposizione del lavoratore funzionalità di sistema in grado di attivare risposte automatiche alle mail; se invece il dipendente manca per malattia, quindi assenze non programmata, e vi è il bisogno di accedere alla casella email, il dipendente può delegare un collega di fiducia con lo scopo di selezionare solo le email inerenti al lavoro.

2.3.4 Sanzioni a carico del datore di lavoro

Il datore di lavoro è soggetto a sanzioni amministrative se non rispetta la legge sulla *privacy* e i principi della delibera n.13 del 1 Marzo 2007, nonché le norme sulla riservatezza e il trattamento dei dati sensibili.

Egli è tenuto a compilare un documento programmatorio per la sicurezza prescritta dal D.Lgs. 196/2003. Tale documento contiene delle procedure, le cosiddette "**misure minime di sicurezza**", a cui tutti i soggetti coinvolti devono attenersi per garantire la sicurezza dei dati e il loro trattamento, secondo principi di correttezza e liceità.

L'adempimento è obbligatorio per tutti gli enti che trattano dati sensibili e dati giudiziari.

La mancata osservanza delle disposizioni dettate dalla normativa sulla *privacy* comporta l'applicazione di severe sanzioni amministrative.

Per non imbattersi in sanzioni amministrative è opportuno affidarsi a consulenti preparati in materia, ed è opportuno che gli adempimenti non vengano fatti in modo superfluo e non idoneo alla struttura dell'impresa.

Capitolo terzo

3.1 La normativa vigente e la giurisprudenza

3.1.1 La delibera del Garante numero 13 del 1° marzo 2007

Le problematiche precedentemente esposte relative all'utilizzo, da parte dei lavoratori, delle risorse informatiche dell'azienda per fini personali e il relativo controllo da parte dei datori di lavoro, hanno fatto emergere la necessità di un intervento da parte del Garante per la protezione dei dati personali, volto a chiarire taluni aspetti legati, prevalentemente, al bilanciamento tra controllo e riservatezza.

Il Garante è intervenuto in materia con la delibera n. 13 del 1° marzo 2007, con lo scopo di prescrivere ai datori di lavoro alcune misure, opportune o necessarie, finalizzate ad armonizzare le esigenze di controllo con le norme relative al trattamento dei dati personali, in relazione all'utilizzo della posta elettronica e della rete internet all'interno dei luoghi di lavoro.

Innanzitutto viene posto, a carico del datore di lavoro, un generale obbligo relativo al buon funzionamento e al corretto impiego della rete internet e della posta elettronica, sia mediante la definizione delle modalità di utilizzo di tali sistemi, sia mediante la predisposizione di misure di sicurezza tese a prevenirne gli utilizzi indebiti; sostanzialmente il Garante ritiene che gravi in capo al datore di lavoro l'informazione e la predisposizione di ogni misura idonea ad evitare un abuso degli strumenti informatici.

La delibera riprende poi tre principi, ritenuti di carattere cogente, espressamente indicati nel D.lgs 196/2010 (noto anche come Codice in materia di protezione dei dati personali), relativi ai presupposti e alle modalità di utilizzazione dei dati personali, imponendone al datore di lavoro il rispetto in ogni situazione in cui si trovi a dovere utilizzare dati personali.

Il primo principio, definito **principio di necessità**, dispone che i sistemi informativi e i programmi informatici debbano essere configurati riducendo al minimo l'utilizzazione di dati identificativi in relazione alle finalità perseguite. Il datore di lavoro è quindi chiamato a promuovere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e a minimizzare l'uso di dati riferibili ai lavoratori. Da un punto di vista organizzativo è quindi opportuno che: si valuti l'impatto sui diritti dei lavoratori, si individui preventivamente a quali lavoratori è accordato l'utilizzo di internet e della posta elettronica e si determini quale ubicazione è riservata alle postazioni di lavoro in modo da ridurre al minimo il rischio di un impiego abusivo. Il Garante, quindi, **indica chiaramente una preferenza nei confronti di misure di prevenzione del rischio di un utilizzo improprio, rispetto ad un controllo successivo sull'operato dei lavoratori.**

Il secondo principio, definito **principio di correttezza**, impone un obbligo di informazione, nei confronti dei lavoratori, in relazione alle caratteristiche essenziali del trattamento dei dati che verrà effettuato. Il trattamento dei dati deve, quindi, ispirarsi ad un canone di trasparenza, come previsto anche dall'art. 4 dello Statuto dei Lavoratori; grava quindi sul datore di lavoro l'onere di indicare,

chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione e in quale misure possano essere esercitati i relativi controlli. Le modalità con cui è possibile adempiere a questi incombenti restano nella discrezionalità del datore di lavoro, il quale dovrà effettuare una valutazione di merito tenendo presente sia le caratteristiche dimensionali dell'azienda, sia quelle relative alla tipologia del lavoro svolto. In questo quadro può, sempre secondo la delibera citata, risultare opportuno adottare un "disciplinare interno", ossia un regolamento applicativo chiaro e senza formule generiche, teso a pubblicizzare in maniera adeguata le informazioni sopra citate.

Il terzo principio, definito **principio di pertinenza**, prescrive che il trattamento dei dati, che deve avere finalità determinate, esplicite e legittime, deve essere eseguito nella maniera meno invasiva possibile della sfera privata dei lavoratori, precisando altresì che le attività di monitoraggio devono essere svolte solo dai soggetti ad esse preposte. Viene quindi posta in risalto la necessità di una graduazione, derivante dal fatto che nell'effettuare i controlli sull'uso degli strumenti elettronici, deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o riservata. **Il controllo è quindi lecito, solo se sono stati rispettati i principi di pertinenza e non eccedenza.** Laddove possibile, è certamente preferibile un controllo su una determinata area o settore, che non permetta di risalire ad un lavoratore specifico. Il Garante impone anche che i dati vengano conservati per un periodo limitato nel tempo, configurando i sistemi software in modo che periodicamente cancellino automaticamente i

dati personali relativi agli accessi, la cui conservazione non risulta assolutamente necessaria.

In conclusione il datore di lavoro, utilizzando sistemi informativi per esigenze produttive e organizzative, o comunque, quando gli stessi si rivelino necessari per la sicurezza sul lavoro, può avvalersi legittimamente di sistemi che consentano indirettamente un controllo a distanza e determinino un trattamento di dati personali riferiti o riferibili ai lavoratori; purché vengano rispettati sia i principi sopra esposti, sia le norme dettate dallo Statuto dei Lavoratori in relazione alle procedure di informazione e consultazione di lavoratori e sindacati.

Restano comunque vietati determinati comportamenti come: la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori al di là di quanto tecnicamente necessario per svolgere il servizio di posta elettronica, la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore, la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo, l'analisi occulta di computer portatili affidati in uso.

3.1.2 Le recenti pronunce della Corte di Cassazione e la sentenza n. 4375/2010

In relazione ai controlli da parte del datore di lavoro, la Corte di Cassazione, si pronunciava con la **sentenza n. 8250/2000**, mediante la quale sanciva l'inutilizzabilità processuale di documentazione probatoria ottenuta in violazione dell'art. 4 dello Statuto dei Lavoratori.

Nel caso di specie la sentenza di merito, confermata dalla Suprema Corte, aveva respinto la domanda proposta da una società proprietaria di un pubblico esercizio nei confronti di una dipendente, intesa al risarcimento dei danni derivanti dalla sottrazione di somme custodite nella cassa, fondata sulla produzione di fotogrammi provenienti da una telecamera a ciruciuto chiuso installata nell'esercizio ove la dipendente prestava lavoro.

La Corte ha sostanzialmente ritenuto che è illegittimo l'uso di una telecamera a circuito chiuso, finalizzata al controllo dei dipendenti, per violazione delle norme a tutela dei lavoratori dettate dall'art. 4 della L. n. 300/1970 e, pertanto, un elemento probatorio ottenuto violando una dispozione di legge, non può essere accolto, da un punto di vista processuale, all'interno del giudizio.

La Corte di Cassazione, con la sentenza n. 4375/2010[19], è recentemente intervenuta sulla questione relativa ai controlli da parte del datore di lavoro ritenendo che i programmi informatici che

[19] 44 Banca dati "Leggi di Italia" 2010

consentono il monitoraggio della posta elettronica e degli accessi ad internet dei dipendenti, sono necessariamente apparecchiature di controllo da assoggettate alle condizioni di cui all'art. 4 dello Statuto dei Lavoratori.

Nel caso di specie una lavoratrice era stata licenziata[20] a causa dell'utilizzo di internet non giustificato da esigenze d'ufficio, rilevato da un programma di controllo informatico denominato "*Super Scout*". Tribunale e Corte d'Appello avevano giudicato illegittimo il licenziamento in quanto i fatti contestati erano stati rilevati e registrati dal suddetto programma in violazione dell'art. 4 dello Statuto dei Lavoratori, con la conseguente inutilizzabilità dei dati acquisiti, ritenendo in ogni caso violate le regole di proporzionalità e gradualità delle sanzioni disciplinari.

La Cassazione ha richiamato il proprio orientamento secondo cui "ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o gli apparecchi di rilevazione di telefonate ingiustificate (v. **Cass. 3-4-2002 n. 4746**). Il detto articolo 4, infatti, sancisce, al suo primo comma, il divieto di utilizzazione di mezzi di controllo a distanza sul presupposto - espressamente precisato nella Relazione ministeriale - che la vigilanza sul lavoro,

[20] Sito web *www.garanteprivacy.it*

ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

Lo stesso articolo, tuttavia, al secondo comma, prevede che esigenze organizzative, produttive ovvero di sicurezza del lavoro possano richiedere l'eventuale installazione di impianti ed apparecchiature di controllo, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso è prevista una garanzia procedurale a vari livelli, essendo l'installazione condizionata all'accordo con le rappresentanze sindacali aziendali o con la commissione interna, ovvero, in difetto, all'autorizzazione dell'Ispettorato del lavoro.

In tal modo, come è stato evidenziato da **Cass. 17-7-2007 n. 15892**, il legislatore ha inteso contemperare l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro, o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi. Con la stessa sentenza, è stato però precisato che l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore per cui, tale esigenza, non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali

comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso. In tale ipotesi si tratta, infatti, comunque di un controllo c.d. "preterintenzionale" che rientra nella previsione del divieto "flessibile" di cui al secondo comma dell'art. 4 citato.

In definitiva, la decisione della Corte d'appello non è censurabile in quanto si è attenuta a tali principi e con motivazione congrua e priva di vizi logici ha affermato che **i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento.**

Ciò risulta evidente laddove nella lettera di licenziamento i fatti accertati mediante il programma "*Super Scout*" sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza sub specie e di aver utilizzato tempo lavorativo per scopi personali.

Da quanto fino ad ora esposto, parrebbe vigere un generale divieto di controllo da parte del datore di lavoro, tuttavia, per quanto questa tesi abbia un'ampia casistica applicativa, vi sono situazioni in cui il controllo è ritenuto in certamente lecito in riferimento ai sopra citati controlli c.d. **"difensivi"**, che fondano le proprie origini in una sentenza del 2002.

Con la sentenza **3 aprile 2002 n. 4746**, la Corte di Cassazione introduceva un concetto fino a quel momento sconosciuto in materia, ossia la classificazione di alcuni tipi di controllo ritenuti "difensivi". Argomentava, infatti, la Corte affermando che, ai fini dell'operatività del divieto di utilizzo di apparecchiature di controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della L. 300/1970, è necessario che il controllo riguardi, direttamente o indirettamente, l'attività lavorativa, mentre **devono ritenersi certamente fuori dall'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore** (c.d. controlli difensivi), quali ad esempio, i sistemi di controllo dell'accesso ad aree riservate o gli apparecchi di rilevazione di telefonate ingiustificate.

Il controllo difensivo sarebbe quindi legittimo in forza del fatto che il divieto di controllo, disposto dallo Statuto dei Lavoratori, farebbe riferimento esclusivamente all'attività lavorativa oggetto del contratto di lavoro e non si espanderebbe ad un generale divieto, imposto al datore di lavoro, di evitare controlli di qualsivoglia condotta dei propri dipendenti.

A pare di chi scrive questa teoria è certamente pregevole perché: se da un lato mira a tutelare la dignità e la riservatezza di ogni lavoratore vietando un controllo diretto a verificare l'attività lavorativa in sé considerata, dall'altro sembra concedere la possibilità, al datore di lavoro, di controllare ed evitare che all'interno della propria azienda possano perpetrarsi condotte illecite con risvolti sia in ambito civile che penale; basti pensare all'ipotesi in cui vengano "scaricati" dalla rete file musicali tutelati dalla L. 633/1941 relativa al diritto d'autore, oppure materiale pedo-pornografico sanzionato ai sensi dell'art. 600

del Codice Penale; questa impostazione consentirebbe un controllo di tipo cautelativo, senza ledere i diritti posti a tutela dei lavoratori.

Dopo avere illustrato l'interpretazione che la Suprema Corte ha dato dell'art. 4 L. 300/1970, sembrerebbe immediato il discrimini esistente tra controlli leciti e illeciti; tuttavia il quadro della complessivo non è così nitido, infatti si è assistito a diverse pronunce che mettono in discussione questa impostazione, come di recente si è avuto modo di notare in relazione alla **sentenza del Consiglio di Stato 19 ottobre**[21] **2009 n. 6373**, con la quale la Giustizia Amministrativa ha stabilito che l'installazione di apparecchi audiovisivi nelle sale del Casinò dove si svolgono particolari giocate (c.d. giochi francesi), non è tale da incidere in modo irragionevole e sproporzionato sul diritto dei lavoratori protetto dall'art. 4, quando siano tese al fine di garantire il regolare svolgimento delle giocate. Le predette installazioni sarebbero giustificate dall'esigenza di assicurare una soluzione certa e immediata di eventuali contestazioni sulle modalità di svolgimento delle giocate, considerando anche il fatto che grava sul gestore del Casinò l'obbligo di assicurare la massima trasparenza e correttezza nelle operazioni di gioco.

In Consiglio conclude poi ricordando che resta fermo il principio per il quale le informazioni acquisite per l'effetto del funzionamento dei detti supporti non possano essere utilizzate in seno al rapporto di lavoro, formando oggetto di contestazioni disciplinari e debbono essere cancellate giornalmente al termine delle operazioni di gioco.

---

[21] Banca Dati "Leggi di Italia" 2010

Conclusioni

E' evidente che la crescita esponenziale[22] di internet e delle tecnologie informatiche hanno radicalmente cambiato la realtà aziendale e le abitudini dei suoi dipendenti.

A tale proposito il datore di lavoro ha dovuto fronteggiare il problema delle misure di sicurezza, onde evitare situazioni come nel caso di perdite di dati aziendali con finalità illecite.

La vigilanza continua o preventiva dell'uso di internet deve garantire dunque, tanto il diritto del datore di lavoro alla protezione dell'organizzazione, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale.

Le tecnologie informatiche e i mezzi che permettono la diffusione di dati personali in tempo reale sono in continua evoluzione, e la necessità di tutelare i diritti fondamentali di un individuo crescono in proporzione a tale diffusione, creando alla giurisprudenza italiana la difficoltà di interpretare le normative emanate dagli organi legislativi.

Un disegno normativo preciso che incastri potere di controllo regolato dal diritto del lavoro e trattamento dei dati non esiste ancora e per questo ci si deve affidare ad un'interpretazione normativa che tenga conto sia delle tutele dei lavoratori (art. 4 legge n.300/1970), sia dei principi giuridici di tutele non che di quelli tecnici contenuti nel codice della *privacy*.

---

[22] *www.adapt.it*

Bibliografia

A.Ciccia, B. Meo. “La privacy nei rapporti di lavoro”, Sistemi editoriali, 2008.

Buttarelli “Banche dati e tutela della riservatezza”, 1997.

S.Niger “Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali”, CEDAM, 2006.

Tiziana Minella “La Privacy”, SIMONE, 2004

G. Finocchiaro e Carla Faralli, “Diritto e nuove tecnologie”, Zanichelli, 2007 .

G. Finocchiaro “Argomenti di informatica giuridica”, CLUEB, 1995.

G. Finocchiaro “Informatica e Pubblica Amministrazione”, CLUEB, 1991.

V. Franceschelli “La tutela della privacy informatica”, Giuffrè editore, 1998.

Sitografia

Autorità Garante per la protezione dei dati personali: *www.garanteprivacy.it*

Camera di commercio: *www.mi.camcom.it*

L'altro Diritto: *www.altrodiritto.unifi.it*

Pinuccia Calia, Ignazio Drudi "Il processo di adozione delle tecnologie informatiche nelle imprese artigiane di servizio: un'analisi multi variata": *www.unibg.it*

Blog di Michele Iaselli "Diritto delle nuove tecnologie" : *micheleiaselli.blogspot.com*

Codice civile online: *www.codice-civile.com*

Corte di cassazione: *www.cortedicassazione.it/Notizie/Notizie.asp*

Legislazione italiana: *www.parlamento.it/parlam/leggi/deleghe/03196dl.htm*